A Remark on Sieving in Biased Coin Convolutions *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

In this work, we establish a nontrivial level of distribution for densities on $\{1, \ldots, N\}$ obtained by a biased coin convolution. As a consequence of sieving theory, one then derives the expected lower bound for the weight of such densities on sets of pseudo-primes.

Introduction.

Over the recent years, there has been an increasing interest in sieving problems in combinatorial objects without a simple arithmetic structure. The typical example is that of finitely generated 'thin subgroups' of linear groups such as $SL_2(\mathbb{Z})$ or $SL_2(\mathbb{Z} + i\mathbb{Z})$. These groups are combinatorially defined but are not arithmetic (they are of infinite index) and as such cannot be studied with classical automorphic techniques. Examples of natural appearances of this type of questions include the study of the curvatures in integral Apollonian circle packings, Pythagorean triples and issues around fundamental discriminates of quadratic number fields and low lying geodesics in the modular surface. (See [2].) The reader may also wish to consult the excellent Bourbaki exposition by E. Kowalski [6] for a detailed account of many of these recent developments around 'exotic sieving'.

*2010 *Mathematics Subject Classification.*Primary 60B99.
†*Key words.* random polynomial, double root, coin convolution, sieving.
‡Research partially financed by the NSF Grants DMS 1301608.

In this paper we consider a slightly different problem but in a somewhat similar spirit. Let $N = 2^m$ and identify $\{1, \dots, N\}$ with the Boolean cube $\{0,1\}^m$ through binary expansion. Denote μ_ρ the probability measure on $\{0,1\}^m$ given by a standard biased coin convolution, i.e. on each factor we take an independent distribution assigning probability ρ to 0 and $1-\rho$ to 1. Consider the resulting distribution on $\{1, \dots, N\}$. For $\rho = \frac{1}{2}$, this is the uniform distribution while for $\rho \to 1$, these distributions become increasingly singular. Our aim is to study some of their arithmetical properties and in particular prove that there is a nontrivial level of distribution no matter how close ρ is to 1, $\rho < 1$. Similar results may also be obtained for g-adic analogues, expanding integers in base g.

Notations.

$e(\theta) = e^{2\pi i\theta}$, $e_q(\theta) = e(\frac{\theta}{q})$.

$c, C =$ various constants.

$A \ll B$ and $A = O(B)$ are each equivalent to that $|A| \leq cB$ for some constant c. If the constant c depends on a parameter ρ, we use $\ll_\rho$. Otherwise, c is absolute.

1 The statement.

Consider the distribution μ on $[1, N] \cap \mathbb{Z}$, with $N = 2^m$, induced by the random variable $\sum_j \xi_j 2^j$ with $(\xi_j), j \geq 0$, be an independent, identically distributed sequence of random variables taking values in $\{0,1\}$, $\mathbb{P}[\xi_j = 0] = \rho$, $\mathbb{P}[\xi_j = 1] = 1-\rho$, $\frac{1}{2} < \rho < 1$. Thus, if $n = \sum_j a_j 2^j$ with $a_j \in \{0,1\}$ the binary expansion, then

$$\mu(n) = \rho^{m-\ell}(1-\rho)^\ell, \quad \text{where } \ell = \sum_j a_j \tag{1.1}$$

Note that for $\rho = \frac{1}{2}$ we obtain the normalized uniform measure on $[0, N]$.

The measure (1.1) has dimension $(1-\rho)\log\frac{1}{1-\rho}$ and hence becomes more irregular for $\rho \to 1$. Our aim is to establish a level of distribution of μ in the sense of sieving theory. Thus, taking $q < N^\alpha$, q square free and α

appropriately small, (since μ is normalized) we may write

$$\begin{aligned}\mu\big[n \leq N : q|n\big] =& \frac{1}{q}\sum_{\lambda=0}^{q-1}\sum_{n=1}^{N} e_q(\lambda n)\mu(n) \\ =& \frac{1}{q} + R_q,\end{aligned} \tag{1.2}$$

where

$$R_q = \frac{1}{q}\sum_{\lambda=1}^{q-1}\sum_{n=1}^{N} e_q(\lambda n)\mu(n).$$

We also assume q odd. The number α is the *sieving exponent*.

Our aim is to obtain a bound of the form

$$\sum_{q<N^{\alpha}}{}' |R_q| = o(1) \tag{1.3}$$

where $\sum'$ sums over q square free and odd.

Theorem 1. *Let the notations be as above. Then μ has sieving exponent $\alpha(\rho) > 0$. In fact, $\alpha(\rho) = O(1-\rho)$ for $\rho \to 1$.*

Sieving pseudo primes is the goal of sieving theory. From standard combinatorial sieve (which also applies to measures instead of sets.) (See e.g. [1], [2], [3], [4]) we have the following result about *r-pseudo-primes* (products of at most r primes).

Corollary 2.

$$\mu(\mathcal{P}_r \cap [0, N]) \sim \frac{1}{\log N} \tag{1.4}$$

with $\mathcal{P}_r = \{r\text{-pseudo-primes}\}, r = r(\rho)$.

2 First estimates.

Let

$$\begin{aligned}R_q =& \frac{1}{q}\sum_{\lambda=1}^{q-1}\sum_{n=1}^{N} e_q(\lambda n)\mu(n) \\ =& \frac{1}{q}\sum_{\lambda=1}^{q-1}\prod_{j<m}\left(\rho + (1-\rho)\, e\left(\frac{\lambda 2^j}{q}\right)\right).\end{aligned} \tag{2.1}$$

Note that

$$|\rho + (1-\rho)e(\theta)|^2 = 1 - 4\rho(1-\rho)\sin^2 \pi\theta. \tag{2.2}$$

Let us consider first the case of small q.

For $\lambda \neq 0 \mod q$, (2.2) implies

$$\left|\rho + (1-\rho)\, e\left(\frac{\lambda 2^j}{q}\right)\right| \leq 1 - \frac{c}{q^2}$$

for $c > 0$ so that (2.1)$< \big(1 - O(\frac{1}{q^2})\big)^m < e^{-C\frac{m}{q^2}} < N^{-c/q^2}$.

One can do better by the following observation.

Let $I \subset \{1, \dots, m\}$ be an arbitrary interval of size $\sim \log q$. Then for $\lambda \neq 0 \mod q$,

$$\max\left\{ \sin^2 \frac{\lambda 2^j}{q}\pi : j \in I \right\} > c \tag{2.3}$$

with $c > 0$ some constant independent of q. Therefore, we also have

$$(2.1) < \big(1 - c(\rho)\big)^{\frac{m}{\log q}} < N^{-\frac{c(\rho)}{\log q}} < e^{-\sqrt{\log N}} \tag{2.4}$$

if $\log q < O\big(\sqrt{\log N}\big)$.

3 Further estimates.

We want to estimate

$$\sum_{q \sim Q} |R_q| \tag{3.1}$$

with $Q < N^\alpha$ and $\log Q \gtrsim \sqrt{\log N}$. It will suffice to show that (3.1)$< Q^{-c}$ for some $c > 0$.

We may assume $\alpha = \frac{1}{t}$ for some large $t \in \mathbb{Z}$ $\big($given in (3.7)$\big)$. Choose $h \in \mathbb{Z}$ such that

$$2^h \sim Q^2. \tag{3.2}$$

Hence

$$h < \frac{2}{t} m < m.$$

Estimate (3.1) using Hölder inequality

$$\begin{aligned}
&\sum_{q\sim Q}{}' |R_q| \\
\le\ &\sum_{q\sim Q}{}' \frac{1}{Q}\sum_{\lambda=1}^{q-1}\prod_{\tau=1}^{t/2}\prod_{j=(\tau-1)h}^{\tau h}\left|\rho+(1-\rho)\,e\Big(\frac{\lambda 2^j}{q}\Big)\right| \\
\le\ &\sum_{q\sim Q}{}' \Big[\prod_{\tau=1}^{t/2}\frac{1}{Q}\sum_{\lambda=1}^{q-1}\prod_{j=(\tau-1)h}^{\tau h}\left|\rho+(1-\rho)\,e\Big(\frac{\lambda 2^j}{q}\Big)\right|^{t/2}\Big]^{2/t} \\
=\ &\sum_{q\sim Q}{}' \frac{1}{Q}\sum_{\lambda=1}^{q-1}\prod_{j=0}^{h-1}\left|\rho+(1-\rho)\,e\Big(\frac{\lambda 2^j}{q}\Big)\right|^{t/2}.
\end{aligned} \tag{3.3}$$

For the last equality, we note that for each τ

$$\begin{aligned}
&\{\lambda 2^j \bmod p : (\tau-1)h \le j < \tau h\} \\
=&\{\lambda 2^j \bmod p : 0 \le j < h\}.
\end{aligned}$$

To finish the estimate, we need the following two lemmas.

Lemma 3. *For all θ, $0<\delta<1$ and*

$$\ell > \frac{\log\frac{1}{\delta}}{\rho(1-\rho)}, \tag{3.4}$$

we have

$$|\rho+(1-\rho)e(\theta)|^{2\ell} \le 1-(1-\delta)\sin^2\pi\theta. \tag{3.5}$$

Proof. Let

$$\gamma = 4\rho(1-\rho)\sin^2\pi\theta.$$

By (2.2),

$$|\rho+(1-\rho)e(\theta)|^{2\ell} = 1-\gamma.$$

We consider the following two cases.

(i). $\gamma > \frac{1}{\ell}\log\frac{1}{\delta}$.

Then

$$(1-\gamma)^\ell \le e^{-\ell\gamma} < \delta < 1-(1-\delta)\sin^2\pi\theta.$$

(ii). $\gamma \le \frac{1}{\ell}\log\frac{1}{\delta}$.

Let

$$\ell_1 = \frac{\ell}{2\log\frac{1}{\delta}} < \ell$$

and estimate

$$\begin{aligned}(1-\gamma)^{\ell} < (1-\gamma)^{\ell_1} < e^{-\ell_1\gamma} &< 1 - \frac{1}{2}\ell_1\gamma \\ &= 1 - \frac{\ell\rho(1-\rho)}{\log\frac{1}{\delta}}\sin^2\pi\theta \\ &< 1 - \sin^2\pi\theta \\ &< 1 - (1-\delta)\sin^2\pi\theta.\end{aligned}$$

(Note that the third inequality is because $\ell_1\gamma < \frac{1}{2}$.) $\square$

Lemma 4. *Let $\gamma < 1/10$ be positive. Then for all θ and $0 < \delta < 1$, we have*

$$1 - (1-\delta)\sin^2\theta \le 1 + \gamma - (1-\delta)\sin^2(\theta+\gamma). \tag{3.6}$$

Proof. Using the identity

$$\sin^2 A - \sin^2 B = \sin(A+B)\sin(A-B)$$

on the difference of both sides of (3.6), we obtain

$$(1-\delta)\big(\sin(2\theta+\gamma)\ \sin\gamma\big),$$

which is bounded by γ. $\square$

Let

$$t > \frac{4\log\frac{1}{\delta}}{\rho(1-\rho)}. \tag{3.7}$$

With $\theta = \lambda 2^j/q$, Lemma 3 implies that (3.3) is bounded by

$$\frac{1}{Q}\sum_{q\sim Q}{}' \sum_{\lambda=1}^{q-1}\prod_{j=0}^{h-1}\left(1-(1-\delta)\sin^2\big(\frac{\pi\lambda 2^j}{q}\big)\right). \tag{3.8}$$

Given Q, let

$$S = \left\{\frac{\lambda}{q} : 0 \le \lambda < q,\ \ q\sim Q\right\} \subset [0,1].$$

We note that $|S| \sim Q^2$ and S is $Q^{-2} \sim 2^{-h}$ separated.

In Lemma 4, taking $\gamma = \pi 2^j \beta'$ with $\beta' \in [0, \beta]$ for some $\beta = O(2^{-h})$ to be specified later, we bound (3.8) by

$$\frac{1}{Q} \sum_{\frac{\lambda}{q} \in S} \prod_{j=0}^{h-1} \left(1 + \gamma - (1-\delta) \sin^2 \left(\pi 2^j (\frac{\lambda}{q} + \beta') \right) \right) \tag{3.9}$$

We will use integration to bound (3.9) by replacing S by $S_\beta = S + [0, \beta]$. Averaging over $\beta' \in [0, \beta]$ gives

$$\begin{aligned} & \frac{1}{\beta Q} \int_{S_\beta} \prod_{j=0}^{h-1} \big(1 + \gamma - (1-\delta) \sin^2(\pi 2^j x) \big) dx \\ \lesssim & \frac{1}{\beta Q} \int_0^1 \prod_{j=0}^{h-1} \big(1 + \gamma - (1-\delta) \sin^2(\pi 2^j x) \big) dx \end{aligned} \quad . \tag{3.10}$$

More precisely, we take

$$\beta = \frac{\delta}{4} \, Q^{-2}, \tag{3.11}$$

(which implies $\gamma < \delta$) and bound (3.10) by

$$\begin{aligned} & \frac{4}{\delta} \, Q \int_0^1 \prod_{j=0}^{h-1} \big(1 + \delta - (1-\delta) \sin^2(\pi 2^j x) \big) dx \\ = & \frac{4}{\delta} \, Q \left(1 + \delta - \frac{1-\delta}{2} \right)^h \\ = & \frac{4}{\delta} \, Q \left(\frac{1+3\delta}{2} \right)^h \\ < & \, Q^{-1/2}, \end{aligned} \tag{3.12}$$

for δ small enough.

Putting (3.3), (3.8)-(3.10) and (3.12) together, we obtain the intended bound on (3.1).

4 Random polynomials with coefficients in $\{0, 1, -1\}$.

The initial motivation for this work came from [7], where one considers biased coin convolution densities for ternary expansions, with probabilities $\mathbb{P}[\xi = 0] = \rho_0$, $\mathbb{P}[\xi = 1] = \rho_1$, $\mathbb{P}[\xi = -1] = \rho_{-1}$ and $\rho_0 \geq \rho_1, \rho_{-1}$. The main problem focused in [7] is to ensure that the set of integers $\{n < N : q^2 | n \text{ for some } q > Q\}$ carries small weight for $Q \to \infty$, which they manage to ensure if q is not too large. The natural problem is whether such restriction is necessary. Clearly, this issue may be rephrased as the sieving problem for square free integers, but with unrestricted level of distribution. (The large values of q are indeed the problematic ones.) While we are unable to provide a definite answer to their question and the main result of this note does not directly contribute, we will point out a simple probabilistic argument leading to the replacement of their condition. Our argument uses virtually no arithmetic structure.

Let $(\xi_j), j \geq 0$, be an independent, identically distributed sequence of random variables taking values in $\{-1, 0, 1\}$. Let $m \geq 1$ and define the random polynomial P by

$$P(z) := \sum_{j=0}^{m} \xi_j z^j$$

In [7], the authors assumed that

$$\max_{x \in \{-1,0,1\}} \mathbb{P}(\xi_0 = x) < \frac{1}{\sqrt{3}} = 0.5773\ldots \tag{4.1}$$

and proved that $\mathbb{P}(P \text{ has a double root }) = \mathbb{P}(P \text{ has } -1, 0 \text{ or } 1 \text{ as a double root })$ up to a $o(m^{-2})$ factor, and $\lim_{m\to\infty} \mathbb{P}(P \text{ has a double root }) = \mathbb{P}(\xi_0 = 0)^2$. One of the open problems they raised at the end of the paper asked whether it is necessary to have assumption (4.1), which enters into the proof mainly through Claim 2.2 in their paper (which is crucial to their results). In this note, we will prove Claim 2.2 under a weaker assumption than assumption (4.1). More precisely, we prove the following.

Assume

$$\max_{x \in \{-1,0,1\}} \mathbb{P}(\xi_0 = x) < 0.7615\ldots. \tag{4.2}$$

Then there exist constants $C, c > 0$ such that for any $B > 0$ we have

$$\mathbb{P}(P(3) \text{ is divisible by } k^2 \text{ for some } k \geq B) \leq CB^{-c}. \tag{4.3}$$

Remark. The bound in (4.2) is the solution to equation (4.10).

Proof. Fix r such that

$$3^r \leq B^2 < 3^{r+1}. \tag{4.4}$$

Claim.

$$\mathbb{P}(P(3) \text{ is divisible by } k^2 \text{ for some } k \in [B, 2B]) \leq 2^{-cr} \tag{4.5}$$

for some constant $c > 0$.

Proof of Claim. We write

$$P(3) = \sum_{j<r} \xi_j 3^j + \sum_{j=r}^{m} \xi_j 3^j.$$

Fix $\xi_r, \dots, \xi_n$, and let $\ell = \sum_{j=r}^{m} \xi_j 3^j$.

If k^2 divides $P(3)$, then

$$\sum_{j<r} \xi_j 3^j \equiv -\ell \bmod k^2.$$

Since $\left| \sum_{j<r} \xi_j 3^j \right| < 3^r/2 \leq k^2/2$, we may denote

$$\ell(k) := \sum_{j<r} \xi_j 3^j \in \left(\frac{-k^2}{2}, \frac{k^2}{2} \right)$$

and let

$$S = \big\{ \ell(k) : k \in [B, 2B] \big\} \subset \big(-2B^2, 2B^2 \big).$$

It follows that

$$\text{the left-hand-side of (4.5)} \leq \mathbb{P}\Big(\sum_{j<r} \xi_j 3^j \in S \Big). \tag{4.6}$$

Let $\sigma_{(k)} = \big(\sigma_{(k)}(j) \big)_{j=0,\dots,r-1} \in \{-1, 0, 1\}^r$ be defined by

$$\sum_{j<r} \sigma_{(k)}(j) 3^j = \ell(k)$$

and let

$$A = \{\sigma_{(k)} : k \in [B, 2B]\} \text{ with } |A| \sim \sqrt{3}^{\,r}.$$

Let δ_j be the indicator function of $j, j = -1, 0, 1$, and denote

$$\rho_j := \mathbb{P}(\xi_0 = j) \text{ for } j = -1, 0, 1, \quad \text{and} \quad \rho := \max_j \rho_j.$$

Denote the product measure on $\{-1, 0, 1\}^r$ by

$$\nu := \bigotimes_{j=0}^{r-1} (\rho_0 \delta_0 + \rho_1 \delta_1 + \rho_{-1} \delta_{-1}).$$

Therefore we have (reasoning given below the display)

$$\begin{aligned}
(4.6) \leq & \sum_{\sigma \in A} \nu(\sigma) \\
\leq & |A|^{1/p} \Big(\sum_{\sigma \in A} \nu(\sigma)^q \Big)^{1/q}, \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} = 1 \\
\lesssim & \sqrt{3}^{\,r/p} \big(\rho_0^q + \rho_1^q + \rho_{-1}^q \big)^{r/q} \\
\leq & \sqrt{3}^{\,r/p} \big(\rho^q + (1-\rho)^q \big)^{r/q} \\
< & 2^{-cr} \quad \text{for some constant} \quad c > 0.
\end{aligned} \tag{4.7}$$

The second inequality is by Hölder, and the third inequality follows from the following estimate.

$$\begin{aligned}
\sum_{\sigma \in A} \nu(\sigma)^q = & \sum_{\sigma \in A} \bigotimes_{j=0}^{r-1} \big(\rho_0 \delta_0(\sigma(j)) + \rho_1 \delta_1(\sigma(j)) + \rho_{-1} \delta_{-1}(\sigma(j)) \big)^q \\
= & \sum_{\sigma \in A} \bigotimes_{j=0}^{r-1} \big(\rho_0^q \delta_0(\sigma(j)) + \rho_1^q \delta_1(\sigma(j)) + \rho_{-1}^q \delta_{-1}(\sigma(j)) \big) \\
\leq & \sum_{a+b+c=r} \binom{r}{a} \binom{r-a}{b} \rho_0^{aq} \rho_1^{bq} \rho_{-1}^{cq} = (\rho_0^q + \rho_1^q + \rho_{-1}^q)^r.
\end{aligned}$$

To finish the proof of the claim, we want to show $(4.7) < 2^{-cr}$ for some constant $c > 0$, i.e.

$$\sqrt{3}^{\,1/p} \big(\rho^q + (1-\rho)^q \big)^{1/q} < 1,$$

and we want to solve

$$t^q + (1-t)^q = \left(\frac{1}{\sqrt{3}}\right)^{\frac{1}{p-1}}, \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} = 1. \tag{4.8}$$

Let $u = \frac{1}{p-1}$ and rewrite (4.8) as

$$\left(t^{1+u} + (1-t)^{1+u}\right)^{1/u} = \frac{1}{\sqrt{3}} \tag{4.9}$$

Let p go to infinity (hence u goes to 0). Then

$$\begin{aligned} & t^{1+u} + (1-t)^{1+u} \\ &= t(1 + u\log t + O(u^2)) + (1-t)(1 + u\log(1-t) + O(u^2)) \\ &= 1 + \big(t\log t + (1-t)\log(1-t)\big)u + O(u^2). \end{aligned}$$

Hence (4.9) becomes

$$\left(1 + \big(t\log t + (1-t)\log(1-t)\big)u + O(u^2)\right)^{1/u} = \frac{1}{\sqrt{3}}.$$

In the limit for $u \to 0$, we obtain

$$e^{t\log t + (1-t)\log(1-t)} = \frac{1}{\sqrt{3}}.$$

Solving

$$t^t(1-t)^{1-t} = \frac{1}{\sqrt{3}}, \tag{4.10}$$

we obtain $t = 0.7615332817632392\cdots$. $\square$

It is possible to exploit somewhat better arithmetical features of the distribution under considerations but gains turn out to be minimal (0.7654 from 0.7615), therefore, will not be elaborated here.

Acknowledgement. The author would like to thank Gwoho Liu for computer assistance.

References

[1] J. Bourgain, A. Gamburd, P. Sarnak *Affine linear sieve, expanders, and sum-product*, Invent. Math., 179(3), 559644, (2010).

[2] J. Bourgain, A. Kontorovich *On the Local-Global Conjecture for integral Apollonian gaskets*, Invent. Math., (2014). arXiv:1205.4416.

[3] J. Friedlander, H. Iwaniec *Opera de cribro*, Amer. Math. Soc., Providence, RI, (2010).

[4] H. Iwaniec and E. Kowalski *Analytic number theory*, Amer. Math. Soc., Providence, RI, (2004).

[5] A. Kontorovich *Levels of Distribution and the Affine Sieve*, Annales de la Faculté des Sci. Toulouse, To appear, (2014)

[6] E. Kowalski *Sieve in Expansion*, Séminaire Bourbaki , 63ème année, no 1028, (2010).

[7] R. Peled, A. Sen, O. Zeitouni *Double roots of random Littlewood polynomials*, preprint, (2014). arXiv:1409.2034.